Implementation of efficient security algorithm for performance improvement and design of ODMRP protocol in VANET environment

A Synopsis Submitted to

Shri Vaishnav Vidyapeeth Vishwavidyalaya

For

DOCTOR OF PHILOSOPHY

In

ELECTRONICS ENGINEERING

By

Prabhat Sharma

PhD Scholar (1805PHDEX04202)

Under the Guidance of

Dr. Swapnil Jain

Assistant Professor, SVITS

Shri Vaishnav Vidyapeeth Vishwavidyalaya

Indore

Research Centre

Shri Vaishnav Institute of Technology and Science

SHRI VAISHNAV VIDYAPEETH VISHWAVIDYALAYA

Ujjain Road, Indore-453111, M.P.

(2019)

A Ph.D. Thesis Synopsis

on

Implementation of efficient security algorithm for performance Improvement and design of ODMRP protocol in VANET environment

Submitted By

PRABHAT SHARMA

(1805PHDEX04202)

Supervisor
Dr. Swapnil Jain
Assistant Professor
S.V.I.T.S., SVVV, Indore

Dean -FDSR
Dr. Santosh Dhar
Dean Research
SVVV, Indore

TABLE OF CONTENTS

Chapter -1	**Introduction**	**……..**	**2**
	1.1 Vehicular Ad-Hoc Network	……	2
	1.2 VANET Security Concept	……	3
	1.3 Attacker's Properties	……	4
	1.4 Motivation	……	6
Chapter -2	**Review of Literature**	**……**	**7**
	2.1 Review	……	7
	2.2 Rationale	……	10
Chapter -3	**Objective of the Study**	**……**	**12**
	3.1 General Objective	……	12
	3.2 Specific Objectives	……	12
Chapter -4	**Methodology**	**……**	**13**
	4.1 Proposed flow chart	……	13
	4.2 Routing Algorithm Steps	……	14
	References	**……**	**15**

CHAPTER 1
INTRODUCTION

1.1 Vehicular Ad-Hoc Network

Vehicular Ad-Hoc Network, or VANET, is a form of mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearest fixed equipment, usually described as roadside equipment.

The VANET used to providing safety and comfort for passenger. In VANET system vehicle need only little electronic gadget inside, which will give Ad-Hoc System connectivity to the travellers inside the vehicle. By this gadget working this system does not require muddled connection and server communication. Every vehicle furnished with VANET gadget will be a hub in the Ad-Hoc organize and can get and transfer others messages through the remote system

In vehicular Ad-Hoc arrange utilizing distinctive ad-hoc organizing innovations, for example, WiFi IEEE 802.11 b/g, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for simple, precise, successful and straightforward communication between vehicles on unique versatility.

The principal approach—called layered methodology and portrayed in Fig. 1(a) endeavours to hold the request of functions and protocol layers with well-characterized interfaces between them. It adapts framework functionalities to the necessities of a VANET communication framework coming about, e.g., in protocol layers for single-jump and multi-bounce communication. The limitations and firmness of traditional system stacks when utilized in ad hoc networks are notable. E.g., each layer is executed as an independent module with interfaces (SAPs) only to the abovementioned and underneath layers. Consequently, protocols can not effectively get to state or metadata of a protocol on an alternate layer what makes information aggregation troublesome. In addition, some of VANET-explicit functions don't fit into the traditional layered OSI model, for example, those for system soundness and control, and can't be extraordinarily allocated to a specific layer. It is likewise significant that each layer gets to outer information independently with no common interface which may lead to issues when this information impacts protocol flow.

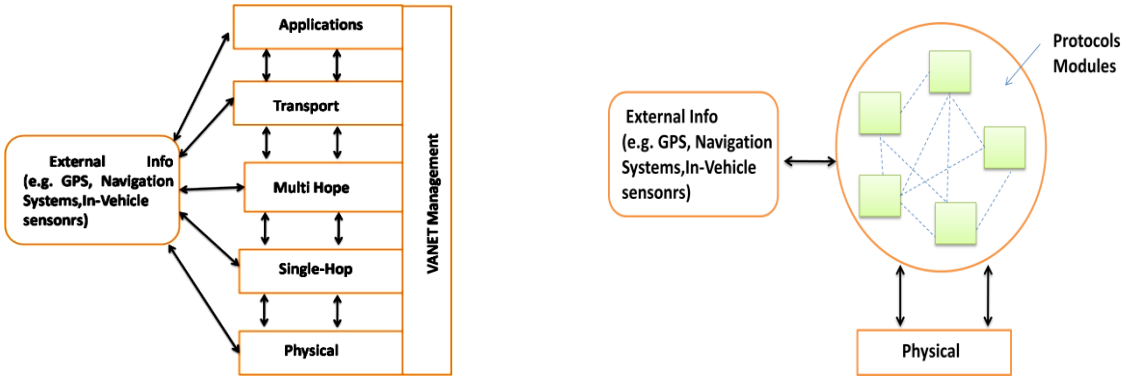

Figure 1: (a) Layered approach (b) Un- Layered approach

The second un-layered methodology would be the after-effect of fitting a totally different framework to the requirements of VANETs' principle centre, i.e., wellbeing applications. Having exact specifications of these applications and willing to utilize the 'probabilistic' direct in the most productive way leads to have a profoundly coupled arrangement of protocols. In this manner, all application and communication protocols are set in one single coherent square directly over the physical interface and connected to the outer sensors (Fig. 1-b). Inside this square, all protocol components are modularized with the end goal that there are no restrictions for interaction, state information is subjective open. Note however, that this 'engineering' acquires a high plan multifaceted nature because of subjective and complex interactions of their modules. This makes protocol specification a confounded work thus, once structured turns into an amazingly firm framework for different kinds of application. Likewise it is tough to methodically maintain a strategic distance from control circle, what is fairly simple in the layered methodology with its tidy top-down or bottom-up packet traversal. While the two methodologies would surely be feasible

1.2 VANET Security Concept

VANET experience the ill effects of different assaults; these assaults are examined in the accompanying subsections:

1. Voracious Drivers: Selfish drivers endeavouring to expand their pick up by making trust a congested way to their goals, and thus smother activity by assaulting the directing components. Snoops drivers endeavouring to profile drivers and concentrate their distinguishing data. Pernicious Snoops can even track vehicle areas and decide the personalities of drivers by comparing them to the house or work destinations.

2. Pranksters: Drivers endeavouring to incapacitate applications or keep data from achieving others vehicles. Such assaults are indicated by Denial of administration assaults/ Denial of Service Attack (DOS).

3. Pernicious Attackers: Drivers intentionally endeavouring to make hurt by means of the accessible applications inside the system. A few assaults concentrate on harming traded information between vehicles, for example, message manufacture, concealment or change. Sybil attack has a place additionally with this class.

4. Mechanical Insiders: If vehicle producers are in charge of securing interchanges inside VANETs, representatives can uncover secret information to noxious elements.

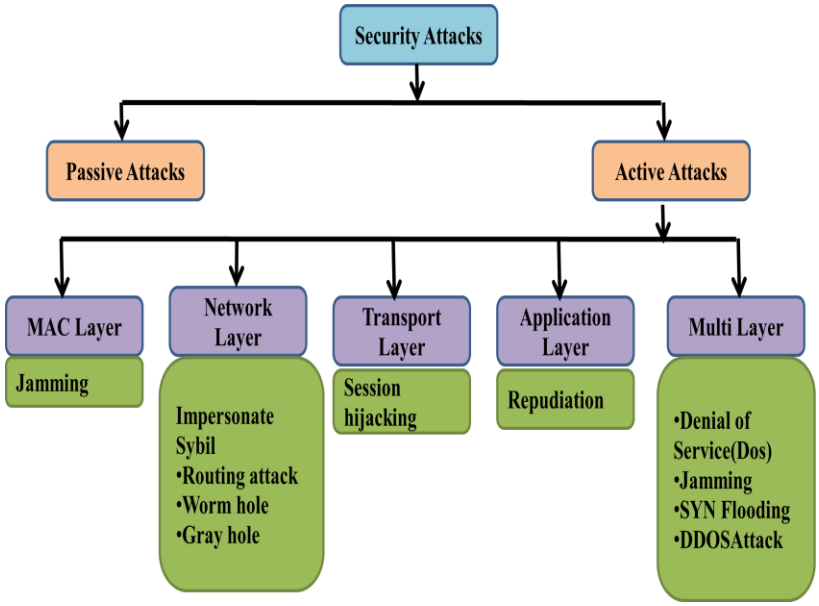

Fig 3.1 Classification of attacks based on Layers

1.3 Attacker's Properties

Aggressor make issue in the system by getting full access of correspondence medium DSRC. Here it is examining a few properties and capacity of the aggressors which has been said in thinks about.

1. Scope Area: Attacker could cover the primary territory of street, and it relies upon the idea of the assaults. Fundamental level assailant has controlled one DSRC channels and covers the scope of at most 1000 meters however the expanded level aggressors are more sorted out and cover more territory utilizing of hundred DSRC channels.

2. Specialized Expertise: Technical mastery of the aggressor makes them more grounded for making assaults in the system. Assailant having capacity to separates the program code and mystery keys of the figuring stage of OBU and RSU by propelling physical assaults.

1.3.1 Types Of Attacks

1. Sticking: The jammer purposely produces meddling transmissions that avoid correspondence inside their gathering range. In the VANET situation, an assailant can moderately effectively segment the system, without trading off cryptographic components and with constrained transmission control.

2. Hub Impersonation Attack: Each vehicle has a novel identifier in VANET and it is utilized to confirm the message at whatever point a mischance occurs by sending incorrectly messages to different vehicles. At the point when police recognize the driver as it is connected with driver's character, assailant changes his/her personality and basically declines it.

3. Sybil Attack: Sybil attack so has a place with the top notch. In Sybil assault, the aggressor sends various messages to different vehicles and each message contains distinctive manufactured source personality (ID). It gives figment to other vehicle by sending some wrong messages like automobile overload message. The goal is to uphold different vehicles headed straight toward leave the street for the advantages of the aggressor.

4. Directing assault: Routing assaults are the assaults which abuses the helplessness of system layer steering conventions. In this sort of assault the assailant either drops the bundle or irritates the steering procedure of the system.

Following are the most widely recognized directing assaults in the VANET:

(i) Black Hole assault: In this sort of assault, the assailant right off the bat pulls in the hubs to transmit the bundle through itself. It should be possible by persistent sending the malevolent course answer with new course and low jump tally. In the wake of drawing in the hub, when the parcel is sent through this hub, it noiselessly drops the bundle.

(ii) Worm Hole assault: In this assault, a foe gets bundles at one point in the system, burrows them to another point in the system, and after that replays them into the system starting there.

(iii) Gray Hole assault: This is the augmentation of dark opening assault. In this sort of assault the malignant hub acts like the dark hub assault however it drops the bundle specifically. This determination can be of two sorts one is malevolent hub can drop the bundle of UDP while the TCP parcel will be sent. Another is pernicious hub can drop the parcel based on probabilistic conveyance.

(iv) Session Hijacking: Most validation process is done toward the begin of the session. Subsequently it is anything but difficult to seize the session after association foundation. In this assault aggressors take control of session between hubs.

(v) Revocation: The principle risk in disavowal is refusal or endeavor to dissent by a hub associated with correspondence. This is not the same as the imitate assault. In this assault at least

two element has normal personality consequently it is anything but difficult to get vague and thus they can be revoked.

(vi)Refusal of Service: DoS assaults are most noticeable assault in this classification. In this assault aggressor keeps the true blue client to utilize the administration from the casualty hub. DoS assaults can be done from various perspectives.

(a) Jamming: In this strategy the assailant detects the physical channel and gets the data about the recurrence at which the recipient gets the flag. At that point he transmits the flag on the channel with the goal that channel is stick.

(b) SYN Flooding: In this instrument expansive no of SYN ask for is sent to the casualty hub, mocking the sender address. The casualty hub send back the SYN-ACK to the mock address yet casualty hub does not receive any ACK parcel consequently. This outcome too half opens association with handle by a casualty hub's support. As an outcome the true blue demand is disposed of.

(c) Distributed DoS assault: This is another frame Dos assault. In this assault, different assailants assault the casualty hub and keeps authentic client from getting to the administration.

1.4 Motivation

In general, protocol architecture achieves for communication among network nodes and provides the framework for implementation. When designing the communication suit for VANETs two approaches can be taken: First, following the traditional approach, the overall functionality could be de-composed and organized in layers such that at the protocols fulfill small, well-defined tasks and form a protocol stack as in TCP/IP and OSI. Second, one could try to build a customized solution that meets the requirements of VANETs with such non-layered.

The motivation of present work is to show VANET simulation using protocol and to show cryptography that yields great efforts in secure communication. In the existing work a hybrid technique is presented which at first define all parameters and develop algorithm which can achieve desired result. The work is upheld by broad recreation comes about which show the adequacy of the proposed techniques in finding a close ideal arrangement.

CHAPTER 2
REVIEW OF LITERATURE

2.1 Review

Tahani gazdar et al., [1] Trust foundation in vehicular extraordinarily designated frameworks is a troublesome task due essentially to the quick of vehicles, the long separations, and the framework topology components. Moreover, applications setting grow quickly while the lifetime authenticity of information messages is short. In this work, creator set up another conveyed trust preparing framework custom-made to VANETs credits and significance to clarify the recently mentioned challenges. The proposed structure depends on the examination of the quick experience between neighboring vehicles without using any suggestion system.

Yanbing Liu et al., [2] The Internet of Vehicles (IoV) plans to give another supportive, pleasant, and safe driving way, and in this manner enables cunning transportation through remote correspondences among road side units, on-board units (OBUs), telephones, and various gadgets inside a vehicle. Nonetheless, basically extending dependence on remote correspondence, control, and handling innovation makes IoV dynamically feeble against potential ambushes, for instance, remote interruption, control, and direction following. As such, compelling validation courses of action envisioning unapproved visitors ought to be directed to adapt to these issues. Therefore, in this work, creator propose, focus on the security and protection sparing by structure up a twofold verification conspires for IoV as demonstrated by its different situations. In any case, the OBU self-makes an obscure personality and temporary encryption key to open a validation session. Second, the legitimacy of the vehicle's real and baffling personality can be confirmed by trust master (TA).

Danda B. Rawat et al., [3] Internet of Vehicles (IoV) is seen as a creating perspective for related vehicles to trade their information with various vehicles using vehicle-to-vehicle (V2V) exchanges by forming a vehicular uniquely selected frameworks (VANETs), with roadside units using vehicle-to-roadside (V2R) correspondences. IoV offers a couple of advantages, for instance, road security, traffic proficiency, and infotainment by sending front line traffic information about cutting-edge traffic. For instance, IoV is seen as an innovation that could help decline the amount of passing realized by road setbacks, and reduce fuel costs and travel break and about.

L. Liu et al., [4] Because of the dynamic topology, high versatility of hubs, and confounded divert environments in urban zones, existing routings strategies are defenceless to visit interface interruptions and channel congestions. To address these issues, a Quality of Forwarding (QoF)-

based dependable geographic routing (QFRG) in urban vehicular ad hoc networks (VANETs) is proposed, where the best course is dictated by ensuring the QoF and fulfilling the connection dependability prerequisite. Two hypothetical models for QoF and connection unwavering quality investigation are first exhibited. Mulling over the transmission cost and the packet conveyance proportion, the QoF is, at that point, utilized to give the quantitative evaluation to the road sections through the displayed road weight evaluation (RWE) plot, which considers the effect of the overall position of connections on the system execution. Next, to oblige the system size of a urban city, the city map is isolated into littler matrix zones. In light of the position of the destination, diverse transmission systems are introduced for packet sending. The broad simulations demonstrate our protocol's prevalence in both transmission delay and packet conveyance proportion contrasted and the current plans.

G. Sun et al., [5] with the improvement of vehicle networks, the information transmission between vehicles is winding up progressively significant. Numerous applications, especially with respect to security, depend on communication between vehicles. These applications have severe necessities for factors, for example, the nature of communication among vehicles and the time delay. Numerous hypothetical communication protocols overlook the nearness of structures or different snags that are available amid viable use, particularly in urban regions. These deterrents can make a signal fade or even square direct communication. Numerous vehicles are often left at the roadside. As a result of their location, these left vehicles can be utilized as transfers to successfully lessen the shadowing impact brought about by deterrents and even tackle communication issues. In this work, creator exhibited left vehicle-right hand-off routing communication in vehicle ad hoc networks. Creator propose an effective left vehicle associate hand-off routing calculation that is made out of four sections: an occasional Hello packet trade instrument, competitor transfer list update, communication connect quality evaluation, and hopeful hand-off rundown selection. Simulation results uncover evident advantages for lists, for example, the nature of communication, achievement rate, and time delay.

Y. Xia et al., [6] Vehicular Ad-hoc Networks (VANETs) require dependable information dissemination for time-touchy open wellbeing applications. A proficient routing protocol assumes a fundamental job to accomplish satisfactory system execution. It is outstanding that routing is a difficult issue in VANETs because of the quick changing system typology brought about by high portability at the two ends of transmission. In addition, under urban environment, there are two non-irrelevant factors in routing protocol plan, the non-uniform vehicle distribution brought about by traffic lights, and the system congestion because of high traffic request in surge hours. In this work,

creator proposed an avaricious traffic light and queue aware routing protocol (GTLQR) which mutually considers the road connectivity, channel quality, relative separation, and lining delay to ease the packet misfortune brought about by vehicle grouping at the intersection and parity the traffic load among vehicles. Through execution evaluation, creator demonstrates proposed protocol beats both TLRC and GLSR-L as far as packet conveyance proportion and end-to-end delay.

G. Araniti et al.,[7] Vehicular Ad-hoc Networks (VANET) is a one of a kind class of Mobile Ad-hoc Network (MANET), which guarantees prospect later on Clever Transporting Framework by giving between vehicle correspondence of road reconnaissance, traffic data, road condition and so forth. Notwithstanding, the high hubs versatility, visit network change topology, temperamental network and little inclusion issues in the VANET usage propels for a steady plan of cloud bunching calculation. This paper propose a framework that consolidates the traditional 802.11p standard VANET networks with LTE networks to shape a half breed Cloud-VANET that gives low network overhead a high versatility the board and high inclusion in VANET networks. This methodology empowers VANET to have high transfer speed alongside un-interruptible information availability by diminishing the information bundle misfortune and SNIR misfortune proportion over the network. The OMNET++ and SUMO traffic generator has been utilized to reproduce the network situation. Recreation results demonstrates that half and half VANET design improve the general network dependability and execution.

khalid abdel et al., [8] Vehicular Ad-hoc NETworks (VANETs) are being considered as one of the empowering innovations to maintain a strategic distance from road mishaps by enabling the vehicles to share the traffic-related data among themselves. Additionally, the VANETs can be utilized for traffic the board and infotainment applications. Adaptability, versatility, and multitenancy are a portion of the essential qualities of a VANET which are required to understand the arrangement of VANET benefits effectively. Author deals with a progressive Programming Characterized Network (SDN) based building system for VANET with help of network virtualization which would make the sending of a specific VANET adaptable in time, space and the kind of administrations offered by it. We additionally present the idea of virtual private VANETs (VPVs) to help multitenancy in VANET. This will permit a VANET specialist organization to convey its administrations over a solitary physical foundation (presumably claimed by an outsider) rapidly in a financially savvy way and in confinement to different administrations running on a similar framework however possessed by various specialist organizations.

Khaleel et al., [9] A vehicular ad-hoc network (VANET), is an example of insightful transportation framework that gives vehicle-to-vehicle correspondence supported by road side foundation for in-vehicle excitement and more secure road condition. VANET is portrayed by exceedingly mobile vehicles, foreordained topology and the necessity of dependable time bound message conveyance over mistake inclined shared remote medium. The security arrangements are obliged by these qualities. In this work author talking about the different sort of assault on VANET alongside crossing point assault on obscurity and the security issue that need to remembered while building up any convention to make VANET secure. Re-enactment and results demonstrate that convergence assault is breaking the protection despite the fact that cryptographic and non cryptographic security component is empowered over the VANET.

Albert Wasef et al., [10] Vehicular ad-hoc networks (VANETs) have turned into a rising innovation that can satisfy the interest of advancing associated vehicles and developing requirement for Canny Transportation Framework (ITS). Authentications are utilized to verify vehicular correspondence however the declarations of vehicles should be disavowed if any vehicles are found as getting out of hand hubs. In VANETs, authentication disavowal list (CRL) must be immediately conveyed to every single vehicular hub to keep from unwanted correspondence with the noxious hubs. Be that as it may, because of developing number of the testaments, the measure of CRL constantly increments, and subsequently, it ends up hard overseeing and conveying the CRL in the vehicular networks. Author presents an effective and adaptable plan to convey declaration denial list in the various levelled engineering of VANETs.

2.1 Rationale

Research Issues in Vehicular Ad-hoc Network can be categorize followings-

- Designing adaptive and efficient channel estimation algorithm and Constructing efficient broadcasting algorithms
- Avoiding unnecessary transmissions
- Security and sensor design
- RSU design
- RSU to RSU communication network specifications
- Privacy issues in VANET
- Achieving QoS in VANET

Routing protocol is primary part of VANETs. These protocols give an interface and communication between remote gadgets. The examination holes depend on routing protocol. The principle objective for routing protocol is to give ideal ways between system hubs through least overhead. Many routing protocols have been created for VANETs environment, which can be grouped from numerous points of view, as per various viewpoints, for example, protocols attributes, systems utilized, routing information, nature of administrations, arrange structures, routing calculations, etc.

CHAPTER 3
OBJECTIVES OF THE STUDY

3.1 General Objective

The main objective in this Synopsis is to enhance security system in V2V communication and develop routing protocol.

3.2 Specific Objectives

The specific objectives are:

1. To implement Security algorithm based on cryptographic approach. A combination of Advance encryption standard (AES) and RSA algorithm is used to improve the security.
2. To develop on-demand multicast routing protocol over VANET environment to control the communication efficiently.
3. By implementing ODMRP protocol in VANET environment throughput can be enhanced and packet delivery time can be reduced, So that more nodes can be connected and each node transmits and receive packet faster.
4. In VANET environment ODMRP is used to reduce packet loss and improve packet delivery ratio. Protocol is more efficient than others so it avoid packet loss.

CHAPTER 4
METHODOLOGY

4.1 Proposed flow chart

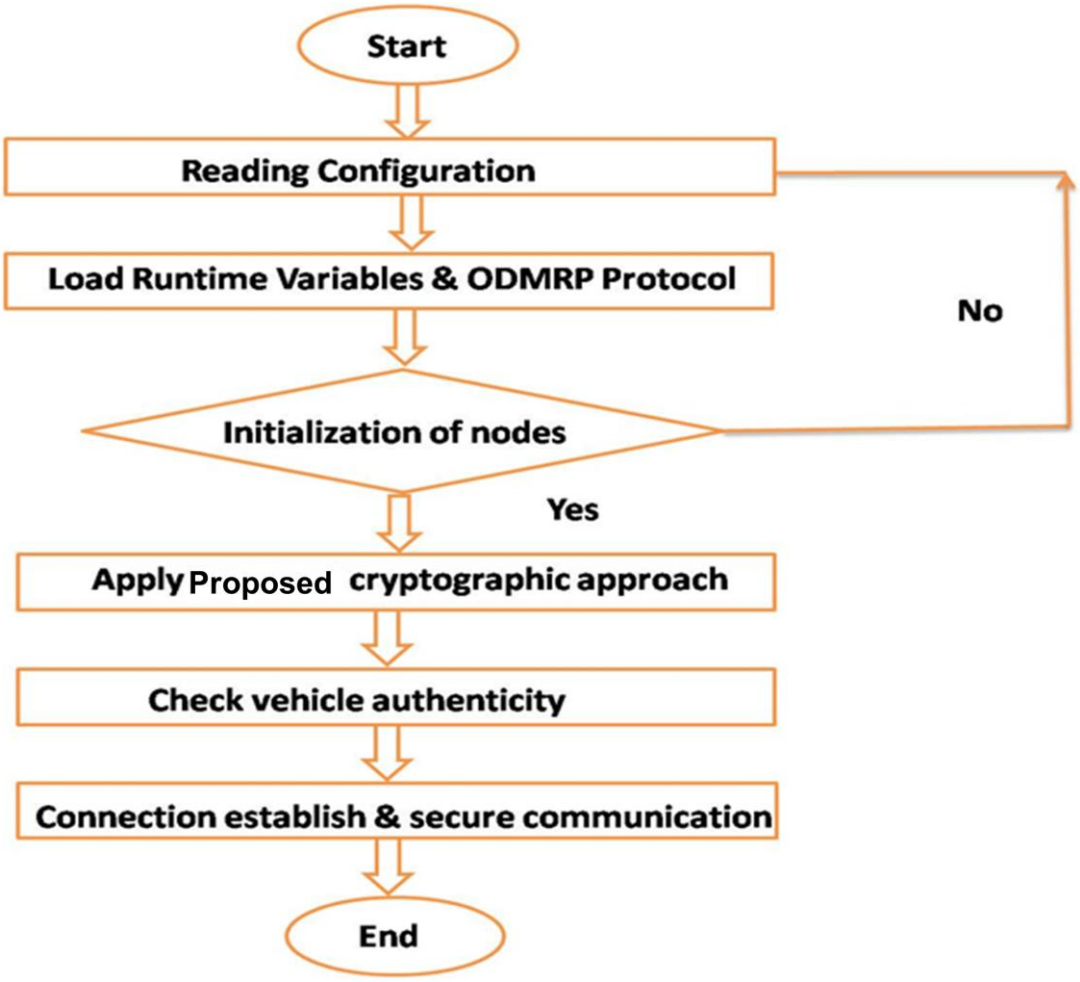

Figure 4.1: Proposed flow chart

4.2 Routing Algorithm Steps

STEP-1: Reading configuration, runtime variables total packets generated in the simulation.

STEP-2: Add topology builder and agent role for Nodes PHY used, MAC protocol, Agents, Applications used in this simulation

STEP-3: Initial nodes, start discrete simulation, update topology matrix, and update plot graph and edges, move node

STEP-4: First we connect listener of the neighbour nodes based on topology, now, process output queue for new packets plot sender related info once.

STEP-5: Generate keys and setup connect with protocol model by using following steps-

1: (Key Setup) Key Generation + Authentication:

- Each party generates RSA Public/Private key-pair.
- Each party exchange their public key with each other.
- Vehicle generates 128-bit AES Symmetric Key, encrypts it with public key received from the RSU and sends this encrypted symmetric key to RSU.
- RSU on receiving the encrypted symmetric key, decrypts it with its own Private Key.

2 : Sending a Message (Encryption Process):

- Vehicle wants to send a message to RSU.
- The Message is encrypted with the AES Symmetric Key.
- The Encrypted Message is encrypted with the RSU Public key..
- Then sent to RSU.

3 : Message Received (Decryption Process) :

- RSU receives [RSU Public key (AES Symmetric Key)+ (AES Symmetric Key Encrypted Message)].
- Decryption with gives (RSU Private Key AES Symmetric Key+(AES Symmetric Key Encrypted Message)).

STEP-6: Check validation of vehicles and connection establish.

REFERENCES

1. Tahani gazdar, Abdelfettah Belghith and Hassan Abutair, "An enhanced distributed trust computing protocol for VANETs" in *IEEE Access*, vol. 6, pp. 380-392, Mar. 2017.
2. Yanbing Liu, Yuhang Wang and Guanghui Chang, "Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm" in *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740-2749, Oct. 2017.
3. Danda B. Rawat, Moses Garuba, Lei Chen and Qing Yang, "On the Security of Information Dissemination in the Internet-of-Vehicles" in *Tsinghua Science and Technology*, vol. 22, no. 4, pp. 437-445, Aug. 2017.
4. L. Liu, C. Chen, B. Wang, Y. Zhou and Q. Pei, "An Efficient and Reliable QoF routing for Urban VANETs With Backbone Nodes" in *IEEE Access, Emerging technologies on vehicle to everything (V2X)*, vol. 7, pp. 38273-38286, Mar. 2019.
5. G. Sun, L. Song, H. Yu, V. Chang, X. Du and M. Guizani, "V2V Routing in a VANET Based on the Autoregressive Integrated Moving Average Model" in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 908-922, Jan. 2019.
6. Y. Xia, X. Qin, B. Liu and P. Zhang, "A greedy traffic light and queue aware routing protocol for urban VANETs" in *China Communications*, vol. 15, no. 7, pp. 77-87, Jul. 2018.
7. G. Araniti, C. Campolo, M. Condoluci, A. Iera and A. Molinaro, "LTE for Vehicular Systems administration: A Survey" in *IEEE Communication Magazine*, vol.51, no. 5, pp. 148-157, May 2013
8. Khalid Abdel Hafeez, Lian Zhao, Bobby Ma, and Jon W. Mark, "Performance analysis and enhancement of the DSRC for VANET's safety applications" in *IEEE transactions on vehicular technology*, vol. 62, no. 7, pp. 3069-3083, Sep. 2013.
9. Khaleel Mershad and Hassan Artail, "A System for Secure and Productive Information Obtaining in Vehicular Specially appointed" in *IEEE exchanges on vehicular innovation*, vol. 62, no. 2, Feb. 2013.
10. Albert Wasef and Xuemin Shen, "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks" in *IEEE transactions on mobile computing*, vol. 12, no. 1, pp. 78-89, Jan. 2013.

11. Jin-Jia Chang, Yi-Hua Li, Wanjiun Liao and Ing Chau Chang, "Urban Vehicular Communications with Traffic –Light Considerations" in *IEEE Wireless communications*, vol. 19, no. 1, pp. 82-88, Feb. 2012.
12. Sandeep Tayal and Malay Ranjan Tripathy, "VANET- Challenges in selection of Vehicular Mobility Model" in *Second International Conference on Advanced Computing & Communication Technologies*, Rohtak, Haryana, India , 7-8 Jan. 2012.
13. Rasheed, S. Gillani, S. Ajmal and A. Qayyum, "Vehicular Ad Hoc Network (VANET): A Survey Challenges and Applications" in *Vehicular Ad-Hoc Networks for Smart Cities, Springer*, pp. 39-51, 2017.
14. M. Ashraf, H. Bilal, I.A. Khan and F. Ahmad, "VANET Challenges of Availability and Scalability" in *VFAST Transactions on Software Engineering*, vol. 10, no. 2, Jul. 2016.
15. T. Taleb, E. Sakhaee, A. Jamalipour, K. Hashimoto, N. Kato and Y. Nemoto, "A Stable Routing Protocol to Support ITS Services in VANET Networks" in *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3337-3347, Nov. 2007.
16. D.K.N.Venkatramana, S.B. Srikantaiah and J. Moodabidri, "SCGRP: SDN-enabled connectivity-aware geographical routing protocol of VANETs for urban environment" in *IET Networks*, vol. 6, no. 5, pp. 102-111, Sep. 2017.
17. M. Zhu, J. Cao, D. Pang, Z. He, M. Xu, K. Xu and H. Zhu, "SDN-Based Routing for Efficient Message Propagation in VANET" in *Wireless Algorithms Systems and Applications: 10 th International Conference WASA 2015 Qufu China*, August 10–12 ,2015, Proceedings, pp. 788-797, 2015.
18. G. Li, L. Boukhatem and J. Wu, "Adaptive Quality-of-Service-Based Routing for Vehicular Ad Hoc Networks With Ant Colony Optimization" in *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3249-3264, Apr. 2017.
19. Y. Ding and L. Xiao, "SADV: Static-Node-Assisted Adaptive Data Dissemination in Vehicular Networks" in *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2445-2455, Jun. 2010.
20. A. O'Driscoll and D. Pesch, "An Infrastructure Enhanced Geographic Routing Protocol for urban vehicular environments" in *IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC)*, Dresden Germany, 02-03 June 2013.
21. X. Lin, X. Sun, X. Wang et al., "TSVC: timed efficient and secure vehicular communications with privacy preserving" in *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4987-4998, Dec. 2008.

22. Falko Dressler, Hannes Hartenstein, Onur Altintas and Ozan Tongus, “Inter-vehicle communication: Quo vadis” in *IEEE Communication Magazine*, vol. 52, no. 6, pp. 170-177, Jun. 2014.
23. Atul B Kathole and Yogadhar Pande, “Survey of topology based reactive routing protocols in VANET” in *International Journal of Scientific & Engineering Research*, vol. 4, no. 6, Jun. 2013.
24. Lili Hu, Zhizhong Ding and Huijing Shi, “An improved GPSR routing strategy in VANET” in *8th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM) , IEEE*, Shanghai China,21-23 Sep. 2012.
25. X. Lin, X. Sun, Pin-Han Ho and X. Shen, “GSIS: A Secure and Privacy –Preserving Protocol for Vehicular Communication” in *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442-3456, Nov. 2007.
26. Degui Xiao, Lixiang Peng ,Clement Ogugua Asogwa and Lei Huang, “An improved GPSR routing protocol” in *International Journal of Advancements in Computing Technology*, vol. 3, no. 5, pp. 132-139,Jun. 2011.